PSEUDO-NOISE SEQUENCE WITH
INSERTION HAVING VARIANT
LENGTH AND POSITION

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable

STATEMENT OF FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not Applicable

5   BACKGROUND OF THE INVENTION

1.   TECHNICAL FIELD

This invention relates in general to communications and, more
particularly, to spread spectrum communications and data encryption.

2.   DESCRIPTION OF THE RELATED ART

10   Spread spectrum communication devices have been used in military and
commercial devices for many years. These devices use noise-like waves to
spread (cover) the information bits so that transmission bandwidth is much
wider than that required for simple point-to-point communication. DS-CDMA
(Direct Spreading Code Division Multiple Access) is a form of spread spectrum
15   which uses a conventional communication waveform and a pseudo-noise (PN)
sequence to transmit information. The PN sequence is commonly generated
using a Linear Feedback Shift Register (LFSR).

In addition to its improved capacity and quality, spread spectrum techniques provide secure communications, since the receiver will generate the same PN sequence as the transmitter. While normal spread spectrum devices are very secure relative to other communication devices, it is possible to determine

5　the polynomial being used to generate the pseudo-noise sequence, since there are a finite number of polynomials for a given sequence length. While third-party deciphering the pseudo-noise sequence may require significant computing power, it is possible that such resources may be available to decipher highly confidential communications.

10　Accordingly, a need has arisen for a method and apparatus for generating a PN sequence which is difficult to decipher.

BRIEF SUMMARY OF THE INVENTION

In the present invention, a communication signal is encrypted using an augmented pseudo-noise sequence. The augmented pseudo-noise sequence is created by generating a plurality of pseudo-noise sequences and combining these

5   pseudo-noise sequences, or portions thereof. The data signal is encrypted using the augmented pseudo-noise sequence.

The present invention provides significant improvements over the prior art. Insertion of one or more segments of arbitrary length from other PN sequences in real time at respective arbitrary points in a PN sequence creates a

10 PN sequence which is almost impossible to decipher. For each period of the augmented PN sequence, the segment parameters and insertion points may change, further increasing the complexity in decrypting the PN sequence.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

5   Figure 1 illustrates a general overview of an augmented PN sequence;

Figure 2 illustrates a preferred embodiment of an augmented sequence which allows for an offset and describes the formation of the augmented sequence;

Figure 3 illustrates a schematic representation of a circuit for generating

10   the augmented sequence of Figure 2;

Figure 4 illustrates a schematic representation of an augmented sequence using multiple segments; and

Figure 5 illustrates use of the augmented pseudo-noise sequence to encode a data signal.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is best understood in relation to Figures 1 - 5 of the drawings, like numerals being used for like elements of the various drawings.

Figure 1 illustrates a general overview of an augmented PN sequence 10
5   for use in spread spectrum devices, or any other device using a PN sequence, formed from two or more PN sequences, PN0 sequence 12 and PN1 sequence 14. The augmented PN sequence 10, PN0 sequence 12 and PN1 sequence 14 could be streams of real or complex numbers, depending upon the application. For example, in a QPSK DS-CDMA system, the augmented PN sequence 10, PN0
10 sequence 12, and PN1 sequence 14 would be sequences of complex numbers, $PN(k)=PN(k)_I+jPN(k)_Q$, where $PN(k)_I$ and $PN(k)_Q$ are one bit values. Many other systems use sequences of real numbers.

A segment 16 of the PN1 sequence 14, which may be all or part of the PN1 sequence, is inserted into the PN0 sequence 12 at an arbitrary position INS_POS
15 of the augmented PN sequence. Segment 16 has arbitrary length SEG_LTH.

In operation, the augmented PN sequence 10 can be used by a data scrambling device in place of the normal, unaugmented PN sequence. Because the augmented PN sequence includes insertion of a second sequence of arbitrary length at an arbitrary position in the augmented PN sequence, determining the
20 polynomial would be exceeding difficult, even using supercomputers.

It should be noted that while the embodiment of Figure 1 illustrates an augmented PN sequence wherein a single segment 16 is inserted into another PN sequence, multiple segments from multiple PN sequences could be inserted into the pseudo-noise sequence, making it even more difficult to decrypt. Further,
25 the starting and ending points of the segment(s) and the insertion point(s) can be modified as often as every period of the augmented PN sequence to further increase complexity.

Figure 2 illustrates a preferred embodiment which allows for an offset and describes the formation of the augmented sequence in greater detail. The offset allows greater flexibility for synchronization within the system. Figure 2 illustrates the Augmented PN sequence 10, PN0 sequence 12, PN1 sequence 14,

5   relative to a reference clock (REF_CT) 20. The reference clock 20 has the same period (AUG_PRD) as the augmented PN sequence 10. OFFSET defines the shift between the starting point (the first word, where a "word" could be a one bit value for a PN sequence of real values or a two bit value for a PN sequence of complex values) of the augmented PN sequence 10 and the start of the reference

10   clock 20. PN0 sequence 12 has a period of PN0_PRD and PN1 sequence 14 has a period of PN1_PRD. One period of the augmented PN sequence 10 is formed from a first segment of PN0 sequence 12 defined by words 0 through INS_IDX0-1 of the PN0 sequence 12, followed by a segment of from PN1 sequence (defined by a segment of SEG_LTH words starting at position BEGIN_IDX1 of the PN1

15   sequence 14), followed by a second segment of PN0 sequence 12 defined by words from position INS_IDX0 to PN0_PRD-1 of the PN0 sequence 12 (i.e., the remaining words of the PN0 sequence 12). Relative to the augmented PN sequence 10, the inserted segment is located in the sequence starting at position INS_POS and ending on RET_POS-1.

20   The output of the augmented PN sequence 10 can begin at any position in the augmented PN sequence 10. In the illustrated embodiment, the output of the augmented PN sequence 10 starts at the position labeled START.

Figure 3 illustrates a schematic representation of a circuit 30 which performs the function described hereinabove. The reference clock signal

25   (REF_CT) is input to one input of a subtractor circuit 32 along with the OFFSET signal. The output of the subtractor circuit 32 is input to a modulo circuit 33 which calculates the remainder of a division of the output of subtractor circuit 32 by AUG_PRD. This remainder is coupled to the first input of dual port

multiplexer 34 and to a first input to subtractor 36. The second input to

subtractor 36 is the segment length (SEG_LTH), which is a constant during a

given period of the augmented PN sequence (although it can change in

subsequent periods). The output of subtractor 36 is coupled to the second input

5   to multiplexer 34. The output of multiplexer 34 coupled to a modulo circuit 35

(generating the remainder resulting from a division of the output of the

multiplexer 34 with PN0_PRD) which calculates idx_A, which specifies a current

index in the PN0 sequence. This index is coupled to the transition matrix 37

which is used by the PN0 pseudo-noise sequence generator 38 (typically a LFSR

10   or similar circuit) to generate the PN0 sequence. An embodiment for the LFSR

and transition matrix are discussed in greater detail in U.S. Ser. No. 09/222,454,

entitled "State Calculation Circuit for Discrete Linear State Space Model" to Gu,

assigned to TEXAS INSTRUMENTS INCORPORATED of Dallas, Texas, filed

December 29, 1998, which is incorporated by reference herein.

15   REF_CT is also coupled adder 40 along with the two's complement of

INS_POS and BEGIN_IDX1(see Figure 2) to adder 40, which sums the three

inputs. The output of adder 40 is coupled to a first input of multiplexer 42 and to

an input of adder 44. The second input of adder 42 is coupled to AUG_PRD (see

Figure 2). The output of adder 44 is coupled to a second input of multiplexer 42.

20   The output of multiplexer 42 is coupled to modulo circuit 46 (generating the

remainder resulting from a division of the output of the multiplexer 42 with

PN1_PRD). The output of modulo circuit 46 is idx_B, which specifies a current

position in the PN1 sequence. This index is coupled to transition matrix 48

which is used by the PN1 pseudo-noise sequence generator 50 to generate the

25   PN1 sequence. The outputs of PN sequence generators 38 and 50 are coupled to

inputs of dual port multiplexer 51. The multiplexer 51 selects between the two

PN sequences to generate the augmented PN sequence.

A bank of comparators 52-57 perform various comparisons used to control multiplexers 34 and 42, PN sequence generators 38 and 50 and multiplexer 51. Comparator 52 determines whether REF_CT is equal to INS_POS. Comparator 53 determines whether REF_CT is equal to RET_POS. Comparator 54 determines

5   whether INS_POS is greater than RET_POS. Comparator 55 determines whether RET_POS is greater than REF_CT. Comparator 56 determines whether REF_CT is greater or equal to INS_POS. Comparator 57 determines whether REF_CT is greater or equal to (INS_POS -INS_IDX0) mod AUG_PRD. The outputs of comparators 54 and 55 are input to AND gate 58 to control multiplexer 42.

10   START is coupled first input gates in OR gates 60 and 62. The output of comparator 52 is coupled to the second input of OR gate 60 and the output of comparator 53 is coupled to the second input of OR gate 62. The output of OR gate 60 is coupled to a first input of AND gate 64 and the output of OR gate 62 is coupled to a first input of AND gate 66. The output of AND gate 64 is coupled to

15   a control port on PN1 sequence generator 50 and the output of AND gate 66 is coupled to a control port on PN0 sequence generator 38. The control ports on sequence generators 38 and 50 load the correct PN states from transition matrices 37 and 48, respectively, and thus reset the sequence generators to a predetermined point in the respective sequence for each period of the

20   augmented PN sequence.

The output of comparator 54 is also coupled to an inverted input of AND gate 68 and to a non-inverted input of AND gate 70. The output of comparator 55 is coupled to an input of AND gate 68 and to an input of OR gate 72. The output of comparator 56 is coupled to an input of AND gate 68 and to an input of

25   OR gate 72. The output of OR gate 72 is coupled to an input of AND gate 70. The outputs of AND gates 68 and 70 are coupled to inputs of OR gate 74. The output of OR gate 74 is the SEQ_SEL signal which controls multiplexer 51 to select which sequence, PN0 or PN1, is output as the augmented PN sequence.

The output of OR gate 74 is also coupled to the inputs of And gates 64 and 66 to make sure that only one of the two PN generators is selected at a given time.

The output of comparator 56 is also output to OR gate 76 through an inverted input and to AND gate 78 through an inverted input. The output of

5   comparator 57 is coupled to a non-inverted input of OR gate 76 and to a non-inverted input of AND gate 78. Subtractor 80 receives INS_POS and INS_IDX0 (see Figure 2) and outputs the difference (INS_POS -INS_IDX0) to modulo circuit 82, which calculates (INS_POS -INS_IDX0) mod AUG_PRD. The output of modulo circuit 82 is coupled to the "B" input of comparator 57 and the sign bit of

10   the difference calculation of subtractor 80 is coupled to an inverted input of AND gate 78 and to a non-inverted input of AND gate 84. The output of OR gate 76 is also coupled to an input of AND gate 84. The outputs of AND gates 78 and 84 are coupled to the inputs of OR gate 86. The output of OR gate 86 is the SEL0 signal which controls multiplexer 34.

15   In operation, the circuit works as follows. The SEQ_SEL signal output from OR gate 74 switches between the outputs of the PN0 sequence generator 38 and the PN1 sequence generator 50. The PN0 sequence is effectively paused while the PN1 segment is inserted into the augmented PN sequence. Switching between the PN0 and PN1 sequences can be accomplished either by pausing the

20   generation of the PN0 or PN1 sequence when it is not selected by multiplexer 51 or by loading the sequence generators at appropriate times to start the sequence at a predetermined point. At steady state, the LOAD0 output from AND gate 66 starts the PN0 sequence at INS_IDX0 after the PN1 segment is complete. The LOAD1 output from AND gate 64 starts the PN1 segment at the BEGIN_IDX1

25   position when the augmented PN sequence has reached INS_POS.

At the initial time, the START signal together with the other control signals decide the first bit of the augmented PN sequence 10 for output, since the

output can begin at any position within the PN0 sequence 12 or segment 16. The

SEL0 signal (the output of OR gate 86) and the SEL1 signal (the output of AND

gate 58), control the multiplexers 34 and 42 to select the correct PN index for T0

and T1, respectively, based on all of the input parameters. The SEL0 signal

5   provides for subtraction of SEG_LTH from the output of the modulo circuit 33

after insertion of segment 16. The SEL1 signal accommodates the situation where

the segment 16 spans the first bit of the augmented PN sequence 10, i.e., where

INS_POS precedes the first bit of the augmented PN sequence 10 and the

RET_POS is after the first bit of the augmented PN sequence 10.

10   Figure 4 illustrates a timing diagram where the PN0 sequence is

augmented by segments from PN1 and PN2. In this case, the segment from PN1

is inserted at INS_POS1 and the segment from PN2 is inserted at INS_POS2.

Any number of PN sequences could be used to generate the augmented PN

sequence. Further, the segments could be inserted into other segments; for

15   example, the PN2 sequence segment could be inserted into the PN1 segment.

         Figure 5 illustrates a block diagram showing the use of the augmented PN

sequence to encrypt a data stream. The pseudo-noise sequence generator 30

outputs a sequence of pseudo-noise words PN(k) to scrambler 90 along with data

stream D(k). Data stream D(k) could be any digital data stream which would

20   benefit from scrambling techniques, such as a digital communication signal or a

native digital signal such as the output of a computing device. In the preferred

embodiment, the scrambler circuit 90 performs an exclusive-or operation on the

digital data stream D(k) and the pseudo-noise sequence PN(k) to generate the

output S.

25   The present invention provides significant improvements over the prior

art. Insertion of a one or more segments of arbitrary length at respective

arbitrary points in a PN sequence creates a PN sequence which is almost impossible to decipher.

   Although the Detailed Description of the invention has been directed to certain exemplary embodiments, various modifications of these embodiments, as well as alternative embodiments, will be suggested to those skilled in the art. The invention encompasses any modifications or alternative embodiments that fall within the scope of the Claims.